

Przełała oszustowi ponad 90- tysięcy złotych!

Data publikacji: 22.12.2022 14:26

Tym razem oszukana metodą „na pracownika banku” została 40-letnia mieszkanka gminy Dębowiec. Za namową fałszywego pracownika banku przełała pieniądze na „konto techniczne”. Kobieta straciła ponad 90 tysięcy złotych! Policjanci i my również, kolejny raz apelujemy, zachowajcie czujność!

□

Kilka dni temu, do 40-latki zadzwonił mężczyzna i podał się za pracownika banku, w którym kobieta posiada konto. **- Na telefonie wyświetlił się numer rozmówcy, dlatego połączenie nie wzbudziło jej podejrzeń. Rzekomy pracownik banku oświadczył, że dzwoni w sprawie weryfikacji danych związanych z kredytem, o który ona ma się starać. Kobieta oświadczyła, że nie złożyła żadnego wniosku o pożyczkę. W tym momencie fałszywy „pracownik banku” poinformował ją, że w takim razie zrobiła to osoba trzecia w jej imieniu, dlatego też natychmiast zawiadamia dział bezpieczeństwa i będzie się z nią kontaktował specjalista tego działu. Chwilę później, w celu „zabezpieczenia” środków pieniężnych i konta, z 40-latką kontakt nawiązał wspomniany „specjalista działu bezpieczeństwa”. Zgodnie z podaną procedurą, żeby „uniknąć” włamania i kradzieży zaoszczędzonych środków, oszuści namówili ją do zainstalowania aplikacji TeamViewer, za pomocą którego mieli zdalny dostęp do komputera. Pokrzywdzona straciła wszystkie swoje oszczędności, które zostały przetransferowane na podane przez oszusta konto** – opisuje sprawę rzecznik prasowy cieszyńskiej policji, st. asp. Krzysztof Pawlik.

40-latka, w ten sam dzień zorientowała się, że padła ofiarą oszustwa. Całą sprawę zgłosiła na policję i do banku. Część z utraconych środków udało się odzyskać.

Po raz kolejny apelujemy o ostrożność i rozwagę podczas telefonicznych rozmów z nieznanymi osobami. Oszuści umiejętnie manipulują rozmową tak, by uzyskać jak najwięcej informacji. W kontaktach z nieznanymi kierujmy się zawsze zasadą ograniczonego zaufania.

Jak oszustwa wyglądają w praktyce wyjaśnia poniżej policja. Proszę pamiętać, że przestępcy modyfikują swoje sposoby, należy więc zachować czujność!

Oszust dzwoni do konkretnej osoby i podaje się za konsultanta bankowego. Numer telefonu, z którego dzwoni fałszywy pracownik placówki bankowej, najczęściej wygląda na oficjalny numerem banku, który można potwierdzić na stronie internetowej. Dzwoniący informuje o niepokojących transakcjach na koncie ofiary. Aby zapobiec i unieważnić te przelewy „konsultant” wybiera różne formy oszustwa- jedną z nich jest zainstalowanie aplikacji AnyDesk lub TeamViewer, która umożliwia mu wykonywanie zdalnych działań na smartfonie lub komputerze rozmówcy. W ten sposób oszust uzyskuje dostęp do urządzenia ofiary i tym samym konta, z którego dokonuje przelewów, a następnie wypłaca zgromadzone na nim środki, a nawet próbuje też zaciągnąć kredyt na konto ofiary.

Drugą formą oszustwa jest wmówienie pokrzywdzonemu, że jest ważnym ogniwem w akcji zatrzymania sprawców włamań na konta bankowe. „Pracownik departamentu bezpieczeństwa” informuje, że zablokował przelew, który usiłowała wykonać inna osoba. „Konsultant” przekonuje pokrzywdzonego, że ten nie widzi podejrzanych ruchów na swoim koncie, ponieważ ma już najprawdopodobniej zmienione przez „włamywaczy” ustawienia i musi czym prędzej wypłacić pieniądze ze swojego konta. Tutaj „ostrzega” swoją ofiarę, że pracownik banku może być w zмовie z przestępcami i też jest obserwowany ponieważ bierze **udział w procederze handlu danymi**. „Konsultant” informuje ofiarę, że wypłacone pieniądze to banknoty „emblemowane”, w związku z czym nie należą do ofiary. Wybrane z konta pieniądze ofiara ma wpłacić w wpłatomacie innego banku, który posiada „odpowiednią licencję”. Z tego tytułu po wpłacie pokrzywdzony namawiany jest do podania kodu BLIK-wówczas rozmówca zapewnia, że kod ten będzie potwierdzeniem wpłaty i jednocześnie podstawą odebrania „zabezpieczonej” gotówki po zakończonej

"akcji".

Pamiętajmy, że przestępcy działają w różny sposób. Modyfikują swój sposób działania, żeby tylko uprawdopodobnić swoją historię. W przypadku oszustwa na pracownika banku mogą dzwonić np. dwie różne osoby. Najpierw otrzymamy informację z oficjalnego numeru konkretnego banku, o tym, że pewna osoba, która w bazach danych widnieje jako oszust, usiłowała zrobić przelew z naszego konta. Przestępca informuje, że w tej sytuacji trzeba podjąć środki zaradcze i pozabezpieczać konta także w innych bankach. Na koniec rozmowy dzwoniący podaje swoje imię i nazwisko oraz numer identyfikacyjny (często zgodny z prawdziwymi danymi), a następnie informuje, że przekazuje sprawę na policję. Po kilku minutach dzwoni inna osoba podająca się za pracownika innego banku, także z oficjalnego numeru banku. Podaje swoje imię i nazwisko oraz numer identyfikacyjny. Nie prosi o podawanie żadnych haseł, ani pinów do konta. Prosi „jedynie” o zainstalowanie aplikacji „AnyDesk, by ochronić środki na koncie. Pokrzywdzeni pobierają wówczas aplikację i postępują zgodnie ze wskazówkami, jakie udzielała im konsultant. Rozmowa niejednokrotnie trwa kilka godzin...

Przestępcy doskonale znają aplikację mobilną i stronę internetową banku. Udzielają też merytorycznych odpowiedzi na wszystkie zadawane pytania, a wręcz przewidują kolejne kroki, jakie należy zrobić. Wiarygodności dodaje fakt, że w telefonie często słychać rozmowy innych konsultantów na tematy bankowe. Dzwoniący mówią płynnie w języku polskim, ale często ze wschodnim akcentem.

Policjanci przypominają i ostrzegają:

- pracownicy banku nigdy nie proszą o podanie loginu i hasła do konta, a tym bardziej kodu autoryzacyjnego SMS lub BLIK;
- nie polecają też instalowania aplikacji, z której mogą wykonywać ruchy na koncie klienta;
- **wykonując JAKIEKOLWIEK operacje finansowe, wykonuj je w placówce bankowej albo z własnej inicjatywy! NIGDY ZA NAMOWĄ osób kontaktujących się telefonicznie!!!!**

O wszelkich próbach wyłudzenia pieniędzy należy natychmiast poinformować policję dzwoniąc na numer alarmowy 112.

red./